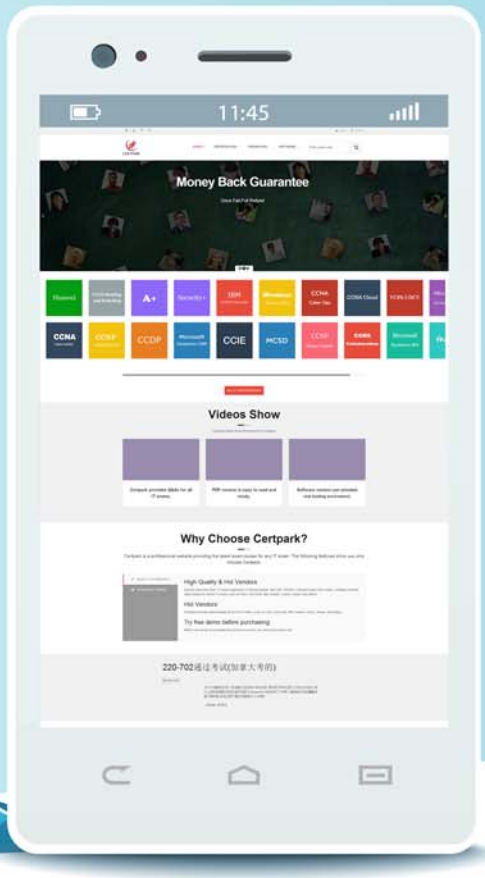
# CERTPARK

## QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!




https://www.certpark.com

**Exam**: **5V0-41.21**

**Title**: VMware NSX-T Data Center 3.1 Security

**Version**: DEMO

1.Which three are required by URL Analysis? (Choose three.)
A. NSX Enterprise or higher license key
B. Tier-1 gateway
C. Tier-0 gateway
D. OFW rule allowing traffic OUT to Internet
E. Medium-sized edge node (or higher), or a physical form factor edge
F. Layer 7 DNS firewall rule on NSX Edge cluster
**Answer:** B,D,F
**Explanation:**
To use URL Analysis, you will need to have a Tier-1 gateway and a Layer 7 DNS firewall rule on the NSX Edge cluster. Additionally, you will need to configure an OFW rule allowing traffic OUT to the Internet. Lastly, a medium-sized edge node (or higher), or a physical form factor edge is also required as the URL Analysis service will run on the edge node. For more information, please see this VMware Documentation article[1], which explains how to configure URL Analysis on NSX.
[1] https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.1/nsxt_31_url_analysis/GUID-46BC65F3-7A45-4A9F-B444-E4A1A7E0AC4A.html

2.What needs to be configured on each transport node prior to using NSX-T Data Center Distributed Firewall time-based rule publishing?
A. DNS
B. NTP
C. PAT
D. NAT
**Answer:** B
**Explanation:**
In order to use NSX-T Data Center Distributed Firewall time-based rule publishing, the NTP (Network Time Protocol) needs to be configured on each transport node. This ensures that the transport nodes have accurate time synchronization, which is required for time-based rule publishing. Additionally, DNS (Domain Name System) and PAT (Port Address Translation) may also need to be configured on each transport node, depending on the desired configuration. References:
[1] https://docs.vmware.com/en/VMware-NSX-T/2.5/com.vmware.nsxt.admin.doc/GUID-E9F8D8AD-7AF1-4F09-B62C-6A17A6F39A6C.html [2] https://docs.vmware.com/en/VMware-NSX-T/2.4/com.vmware.nsxt.admin.doc/GUID-E9F8D8AD-7AF1-4F09-B62C-6A17A6F39A6C.html

3.An NSX administrator is trying to find the dvfilter name of the sa-web-01 virtual machine to capture the sa-web-01 VM traffic.
What could be a reason the sa-web-01 VM dvfilter name is missing from the command output?
A. sa-web-01 VM has the no firewall rules configured.
B. ESXi host has 5SH disabled.
C. sa-web-01 is powered Off on ESXi host.
D. ESXi host has the firewall turned off.
**Answer:** C
**Explanation:**

The most likely reason the sa-web-01 VM dvfilter name is missing from the command output is that the sa-web-01 VM is powered off on the ESXi host. The dvfilter name is associated with the VM when it is powered on, and is removed when the VM is powered off. Therefore, if the VM is powered off, then the dvfilter name will not be visible in the command output. Other possible reasons could be that the ESXi host has the firewall turned off, the ESXi host has 5SH disabled, or that the sa-web-01 VM has no firewall rules configured.
References: [1] https://kb.vmware.com/s/article/2143718 [2] https://docs.vmware.com/en/VMware-NSX-T/3.0/vmware-nsx-t-30-administration-guide/GUID-AC3CC8A3-B2DE-4A53-8F09-B8EEE3E3C7D1.html

4.Which two statements are true about IDS/IPS signatures? (Choose two.)
A. Users can upload their own IDS signature definitions from the NSX UI.
B. IDS Signatures can be High Risk, Suspicious, Low Risk and Trustworthy.
C. Users can create their own IDS signature definitions from the NSX UI.
D. An IDS signature contains data used to identify known exploits and vulnerabilities.
E. An IDS signature contains a set of instructions that determine which traffic is analyzed.
**Answer:** D,E
**Explanation:**
(https://pubs.vmware.com/NSX-T-Data-Center/index.html#com.vmware.nsxt.admin.doc/GUID-AFAF58DB-E661-4A7D-A8C9-70A3F3A3A3D3.html)

5.An organization is using VMware Identity Manager (vIDM) to authenticate NSX-T Data Center users Which two selections are prerequisites before configuring the service? (Choose two.)
A. Validate vIDM functionality
B. Assign a role to users
C. Time Synchronization
D. Configure vIDM Integration
E. Certificate Thumbprint from vIDM
**Answer:** D,E
**Explanation:**
The two prerequisites before configuring the VMware Identity Manager (vIDM) service for NSX-T Data Center are Configure vIDM Integration and Certificate Thumbprint from vIDM. In order to use vIDM for authentication, it must be integrated with NSX-T Data Center, which will involve configuring the vIDM integration service. Additionally, a certificate thumbprint from vIDM must be provided to NSX-T Data Center to enable secure communication between the two services. Time synchronization and assigning roles to users are not necessary prerequisites for configuring the vIDM service.
References: [1] https://docs.vmware.com/en/VMware-NSX-T/3.0/vmware-nsx-t-30-administration-guide/GUID-1B4EA3C9-8F43-4C4F-A86A-BFB0DB6D1A6C.html [2] https://docs.vmware.com/en/VMware-Identity-Manager/3.3/com.vmware.identity.install.doc/GUID-D56A0C0A-52F